CRS EQUIPMENT MAINTENANCE NOTE 58 (for Electronics Technicians)
Maintenance, Logistics, and Acquisition Division
W/OSO321: GSS

SUBJECT	:	CRS Password Modification Procedures
PURPOSE	:	To provide CRS password modification procedures in compliance with Department of Commerce policies.
SITES AFFECTED	:	All CRS sites.
ESTIMATED COMPLETION DATE	:	Quarterly as directed by CRS Password Change Day Policy (see attachment B).
EQUIPMENT AFFECTED	:	All CRS Front-end, Main, and Voice Improvement Processors (FEPs, MPs, and VIP).
SPARES AFFECTED	:	None.
ACCOMPLISHED BY	:	NWS Electronic Systems Analysts.
PARTS REQUIRED	:	None.
SOURCE OF MATERIALS	:	Not applicable.
TOOLS AND TEST EQUIPMENT REQUIRED	:	None.
TIME REQUIRED	:	1 hour total for all processors.
EFFECT ON OTHER INSTRUCTIONS	:	None
AUTHORIZATION	:	The authority for this maintenance procedure is the CRS Password Change Day Policy (see attachment B).
VERIFICATION STATEMENT	:	This procedure was tested and verified at National Weather Service Headquarters, Silver Spring, Maryland (SLVM2).

DISPOSITION OF REMOVED PARTS/MATERIALS	:	Not applicable.
PROCEDURE	:	Attachment **A** provides procedures for implementing this maintenance procedure. Attachment **B** provides CRS Password Change Day Policy.
REPORTING INSTRUCTIONS	:	Report the completed modification using the Engineering Management Reporting System (EMRS) according to the instructions in the NWS Instruction 30-2104, Maintenance Documentation, Part 4 and Appendix G. Include the following information on the EMRS Report: a. An equipment code of **CRSSA** in block 7. b. A serial number of **001** in block 8. c. A maintenance number of **M58** in block 17a. A sample EMRS Report is provided as attachment **C**.

Signature Not Verified

Mark S. Paese

Digitally signed by Mark S. Paese
DN: cn=Mark S. Paese, o=DOC/NOAA/NWS, c=US
Date: 2003.05.13 16:18:54 -04'00'

Mark S. Paese
Director, Maintenance, Logistics, and Acquisition Division

Attachment **A** - Maintenance Procedure
Attachment **B** - CRS Password Change Day Policy
Attachment **C** - EMRS Report Sample

ATTACHMENT A
CRS Password Modification Procedures

General

These procedures detail which CRS user account passwords will be changed and how to change them.

CAUTION

Do not use special characters in any of the CRS user account passwords. Even though the Department of Commerce password management policy specifies the use of at least one number or special character in the password, the CRS application software currently will not allow the use of special characters. The use of a special character in any password will cause the GUI login attempt to fail. Therefore, until this problems is fixed, sites must use at least one number in all CRS passwords.

NOTE:

1. The CRS system must be running in a normal configuration, e.g., 0MP as the Master MP and 5MP as the Shadow MP. All FEPs must be running in a normal configuration, i.e., 4BKUP should not be an active FEP. The CRS and VIP applications must be stopped.

2. The following CRS user accounts are present on all CRS nodes: **root**, **crs**, **admin**, **maint** and **oper**.

3. The **switchmp** user account is only required on the 0MP and 5MP nodes. The **sysadm** user account is only required on the FEP nodes.

4. When changing system passwords, make sure the changes are made on each system node, i.e., 0MP, 5MP, 1FEP, 4BKUP and any remaining FEP nodes. The VIP has only user accounts **root** and **crs** that must be changed. Additionally, the LAN Server **root** user password must be changed.

5. The LAN server (ps8) root password is limited to a maximum of 8 characters. Therefore, if sites choose to have their root passwords match on all processors, they must limit them to 8 characters.

1.1 Preliminary System Setup Procedures

1. Before proceeding, read the entire note.
2. Schedule CRS downtime to perform this procedure. As a conservative estimate, schedule one hour to perform the procedure. This is a conservative estimate. The actual downtime may be less, or it may be more if you encounter problems.
3. Notify the public that CRS (NOAA Weather Radio) will be down during this scheduled time for maintenance.

1.2 Procedure for Changing Passwords on the MPs and FEPs

Check to see if the CRS application is running. If it is, stop the CRS application by clicking the **System** menu and then select **Stop System** and select **OK**. Wait until the application is stopped completely. Check to see if the VIP server is running. If it is, then stop the VIP server by clicking **Stop** on the VIP main interface menu. Then proceed with the following steps.

1. On 0MP open a *UNIX shell* window from the *Maintenance* menu.
2. Log in as the *root* user:

   0MP{admin} **su**

   Enter the root password.
3. Use the UNIX *passwd* command to change the user passwords on the 0MP node. For the exact syntax and usage of the command, use the *man passwd* command string.

   # **passwd root**

   Follow the prompts to change the password.

   # **passwd crs**

   Follow the prompts to change the password.

   # **passwd admin**

   Follow the prompts to change the password.

   # **passwd maint**

   Follow the prompts to change the password.

   # **passwd oper**

   Follow the prompts to change the password.

   # **passwd switchmp**

   Follow the prompts to change the password.
4. Exit the *root* user.

   # **exit**

5. Log into the 5MP node using the *rsh* command:

   0MP{admin} **rsh 5MP**

   Log in as the *root* user:

   5MP{admin} **su**

   Enter the *root* password

6. Use the UNIX *passwd* command to change the user passwords on the 5MP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 1. The passwords should be changed to match the 0MP node passwords.

   # **passwd root**

   Follow the prompts to change the password.

   # **passwd crs**

   Follow the prompts to change the password.

   # **passwd admin**

   Follow the prompts to change the password.

   # **passwd maint**

   Follow the prompts to change the password.

   # **passwd oper**

   Follow the prompts to change the password.

   # **passwd switchmp**

   Follow the prompts to change the password.

7. Exit the *root* user and the 5MP node by typing *exit* twice.

   # **exit**

   5MP{admin} ***exit***

8. Log into the 1FEP node using the *rsh* command:

   0MP{admin} **rsh 1FEP**

   Log in as the *root* user:

   1FEP{admin} **su**

   Enter the *root* password.

9. Use the UNIX *passwd* command to change the user passwords on the 1FEP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 2. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

passwd root

Follow the prompts to change the password.

passwd sysadm

Follow the prompts to change the password.

passwd crs

Follow the prompts to change the password.

passwd admin

Follow the prompts to change the password.

passwd maint

Follow the prompts to change the password.

passwd oper

Follow the prompts to change the password.

10. Exit the *root* user and the 1FEP node by typing *exit* twice.

exit

1FEP{admin} **exit**

11. Log into the 4BKUP node using the *rsh* command:

0MP{admin} **rsh 4BKUP**

Log in as the *root* user:

4BKUP{admin} **su**

Enter the *root* password

12. Use the UNIX *passwd* command to change the user passwords on the 4BKUP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 3. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

 # passwd root

Follow the prompts to change the password.

 # passwd sysadm

Follow the prompts to change the password.

 # passwd crs

Follow the prompts to change the password.

 # passwd admin

Follow the prompts to change the password.

 # passwd maint

Follow the prompts to change the password.

 # passwd oper

Follow the prompts to change the password.

13. Exit the *root* user and the 4BKUP node by typing *exit* twice.

 # exit

4BKUP{admin} **exit**

NOTE: 4. Sites with more than two FEP nodes should change passwords on the remaining FEPs as applicable. See the following steps.

14. Log into the 2FEP node using the *rsh* command:

0MP{admin} **rsh 2FEP**

Log in as the *root* user:

2FEP{admin} **su**

Enter the *root* password.

15. Use the UNIX *passwd* command to change the user passwords on the 2FEP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 5. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

passwd root

Follow the prompts to change the password.

passwd sysadm

Follow the prompts to change the password.

passwd crs

Follow the prompts to change the password.

passwd admin

Follow the prompts to change the password.

passwd maint

Follow the prompts to change the password.

passwd oper

Follow the prompts to change the password.

16. Exit the *root* user and the 2FEP node by typing *exit* twice.

    # **exit**

    2FEP{admin} **exit**

17. Log into the 3FEP node using the *rsh* command:

    0MP{admin} **rsh 3FEP**

    Log in as the *root* user:

    3FEP{admin} **su**

    Enter the *root* password.

18. Use the UNIX *passwd* command to change the user passwords on the 3FEP node. For the exact syntax and usage of the command, use the *man passwd* command string.

NOTE: 6. The passwords should be changed to match the 0MP node passwords where they exist. The sysadm password, which only exists on the FEPs, should be the same on all FEPs.

passwd root

Follow the prompts to change the password.

passwd sysadm

Follow the prompts to change the password.

passwd crs

Follow the prompts to change the password.

passwd admin

Follow the prompts to change the password.

passwd maint

Follow the prompts to change the password.

passwd oper

Follow the prompts to change the password.

19. Exit the *root* user and the 3FEP node by typing *exit* twice.

    # **exit**

    3FEP{admin} **exit**

20. Exit the *UNIX shell* window by typing *exit*.

1.3 Procedure for Changing Root and CRS User Passwords on the VIP

1. Click *Shell* (lower left area of the screen) to open a *Linux shell* window.
2. Type:

   su

3. Enter the *root* password.
4. Type:

   passwd root

   The system prompts: *Changing password for user root.*

5. *New password*: [enter new password here]
6. Re-type new password: [re-enter new password here]

   The system displays: *Password : all authentication tokens updated successfully.*

7. Type:

   passwd crs

   The system prompts: *Changing password for user crs.*

NOTE: 1. Use the same CRS password used in the MPs and FEPs.

8. *New password*: [enter new password here]
9. Re-type new password: [re-enter new password here]

   The system displays: *Password : all authentication tokens updated successfully.*
10. Exit the *Linux shell* window by typing *exit* twice.
11. Click **System Settings** on the VIP main interface menu. The *VIP System Settings* dialog displays.
12. Enter the new CRS password in the text box.

NOTE: 2. Use the same CRS password used in the MPs and FEPs.

13. If you are running VIP version 2.0.2 or earlier, click the **OK**, **Apply** and/or **Close** buttons as necessary to save the settings and exit the window. This procedure is completed. Skip to the next procedure.
14. If you are running VIP version 3.0 or later, click **File** and click **Save**.
15. Select **Options->Setup Wizard** from the *VIP System Settings* dialog box. The *VIPv3.0 setup wizard* window displays.
16. Click **Next**.
17. Click **I understand the above disclaimer** and click **Next**.
18. The *VIPv3.0 setup wizard: Step 3 window* displays.
19. Enter the new CRS password in the *CRS user 'crs' password* text box.

NOTE: 3. Use the same CRS password used in the MPs and FEPs.

20. Keep clicking **Next** until the *VIPv3.0 setup wizard: Finished* window displays.
21. Click **Finish**.

1.4 Procedure for Running */crs/bin/chg_emb_pw.ksh* on 0MP

The new password should be manually changed on 0MP, 5MP, FEPs, and the VIP prior to running the */crs/bin/chg_emb_pw.ksh* script.

NOTE: 1. The CRS and VIP applications must not be running. If the CRS application software is running, stop the CRS application by clicking the **System** menu, selecting **Stop System**, and then selecting **OK**. Wait until the application completely stops. If the VIP application is running, stop the VIP application by clicking **Stop** on the VIP main interface menu.

1. Log in as *root* user
2. Type:

   /crs/bin/chg_emb_pw.ksh
3. The system prompts:

   Have crs password changes been made on all crs processor?(default: y)

   Press **Enter**.
4. The system prompts:

   Change crs embbed user password in /crs/bin/ftp.ksh?(default: y)

   Press **Enter**.

NOTE: 2. Use the same CRS password used in the MPs, FEPs, and VIP.

5. *New password:* [enter new password here]
6. *Re-enter new password:* [re-enter new password here]

   The system prompts:

   INFO: /crs/bin/ftp.ksh sucessfully updated on 0MP

   INFO: /crs/bin/ftp.ksh sucessfully updated on 1FEP

   INFO: /crs/bin/ftp.ksh sucessfully updated on 2FEP (if you have one)

   INFO: /crs/bin/ftp.ksh sucessfully updated on 3FEP (if you have one)

   INFO: /crs/bin/ftp.ksh sucessfully updated on 4BKUP

   INFO: /crs/bin/ftp.ksh sucessfully updated on 5MP
7. Exit the *UNIX shell* by typing *exit* twice.

1.5 Procedure for Changing the LAN Server (ps8) Password

NOTE: 1. The CRS and VIP application software should not be running. If CRS application software is running, then stop the CRS application by clicking the **System** menu, selecting **Stop System**, and then selecting **OK**. Wait until the application completely stops. If the VIP application is running, stop the VIP application by clicking **Stop** on the VIP main interface menu.

1. Open a *UNIX shell* window from the *Maintenance* menu.
2. Type:

   telnet ps8
3. Log in as *root* user (default password is **dbps**)
4. Type:

   newpass
5. The system prompts:

   current password: [enter current password]
6. The system prompts:

   new password: [enter new password]

NOTE: 2. No more than 8 characters are allowed in the password.

7. The system prompts:

   repeat new password: [re-enter new password]
8. Type:

   exit
9. Start the CRS application software by clicking the **System** menu, selecting **Start System**, and then selecting **OK**. Start the VIP application by clicking **Start** on the VIP main interface menu.

1.6 Procedure for Changing the CRS User Password in the */data/fxa/workFile/nwr/nwr.cfg* File on the AWIPS DS1 Node

AWIPS System Assumptions

The */data/fxa/workFiles/nwr/nwr.cfg* file has been correctly configured on the site DS1 node. The file should contain, in strict order, the following information: CRS user name, CRS user

password, and the interface type **LAN**. The CRS user password must be changed to match that used in CRS. See the following example:

```
ds1-nmtw{awipsusr}2: cat /data/fxa/workFiles/nwr/nwr.cfg
crs
XXXXX [Verify the correct crs user password here]
LAN
ds1-nmtw{awipsusr}3:
```

NOTE: Based on your system configuration, change your CRS password on every AWIPS node where the *nwr.cfg* file exists. For example, if you run transferNWR on workstations to ftp messages to CRS, the CRS password must be changed there as well. If you are unsure of your specific configuration, please check with the AWIPS focal point.

ATTACHMENT B
CRS Password Change Day Policy

Effectively immediately, in compliance with the new Department of Commerce (DOC) Password Policy, CRS will have a password change day each quarter. The change days will be February 15, May 15, August 15, and November 15. To allow for scheduling of appropriate staff needed to make the changes and to allow for potentially life-threatening weather situations, each Weather Forecast Office (WFO) will implement the password changes within 2 weeks of the password change day. The first password change day will be May 15, 2003. Please change ALL passwords on ALL accounts on all MPs, FEPs, the VIP, and the LAN server. The DOC security policy requires that a different password be used for each account. However, it is permitted to retain the same passwords for the same accounts on different processors, e.g., the CRS user password is the same on both 0MP and 5MP.

CRS is compliant with some and parts of some of the 13 password requirements described below. Other requirements will have to wait for future software builds for full compliance; still others make no sense for implementation in CRS. **For the purposes of the change day policy, sites must ensure compliance with requirements 1, 4, 8, and 9 described below.** The Meteorologist in Charge (MIC) at each office will designate a staff member to be responsible for enforcing the four requirements. Requirements 1, 8, and 9 are self-explanatory; for the purposes of CRS, requirement 4 means that userid/password information for the CRS components will be maintained in a locked container in the operations area of the office that is staffed 24 hours a day, 7 days a week, so that, if necessary, the CRS Help Desk may be given the password for remote troubleshooting.

Listed below are the mandatory DOC password requirements.

Passwords must be created consistent with the following criteria:

1. Passwords must have at least eight (8) non-blank characters and comply with the following guidelines:
    a. At least one of the characters must be from the alphabet (uppercase or lowercase).
    b. At least one of the characters must be a number (0-9) or a special character (e.g., ~, !, $, %, ^, and *). **[See Caution note under "General" on page A-1 of attachment A regarding the use of special characters in CRS passwords.]**
    c. Six of the characters may only occur once in the password (e.g., "AAAAAAA1" is not acceptable, but "A%rmp2g3" and "A%ArmA2g3" are acceptable).
    d. Passwords must ***not*** include any of following:
        1) Vendor/manufacturer default passwords;
        2) Names (e.g., system user names, family names);

3) Words found in dictionaries (i.e., words from any dictionary, spelled forward or backward);

4) Addresses or birthdays, or common character sequences (e.g., 3456, ghijk, 2468).

e. Vendor-supplied default passwords, such as SYSTEM, Password, Default, USER, Demo, and TEST, must be replaced immediately upon implementation of a new system.

NOTE: With the implementation of CRS Build 9.0/VIP Build 3.0.2 in June 2003, the new VIP operating system, Linux 7.3, will include some of the password checking described above. Sites should pay close attention to the requirement to restrict the use of words from dictionaries. In fact, Linux 7.3 *prevents* the use of passwords based on a dictionary word Experience shows that the best password is based on the random generation of characters.

2. Systems or applications that have multiple passwords for different levels of access or authentication must have unique passwords for each level.

3. Passwords must be protected to prevent unauthorized use. Specifically:

   a. Passwords must not be shared except in emergency circumstances or when there is an overriding operational necessity as documented in an operating unit System Security Plan. Once shared, passwords must be changed as soon as possible.

   b. Group passwords (i.e., a single password used by a group of users) must not be used without some other mechanism that can ensure accountability (such as separate and unique network User IDs).

   c. Group passwords must not be shared outside the group of authorized users and must be changed when any individual in the group is no longer authorized. Group passwords must never be re-used.

   d. Passwords that need to be shared because of an overriding operational necessity, as well as group passwords, cannot be used to control access to other IT systems or applications on IT systems.

4. Passwords in readable form (e.g., written on paper) must be kept in a safe location and must not be stored in a location accessible to others. For example, safe locations include storage in a locked container accessible only by the user.

5. IT systems and workstations must not display or print passwords as they are entered.

6. User applications must not be enabled to retain passwords for subsequent re-use, or be configured to bypass authentication mechanisms. For example, Internet browsers must not be enabled to save passwords for re-use.

7. Passwords must not be distributed through non-encrypted electronic mail or through voicemail, nor be left on answering machines.

8. Passwords must be changed as follows:

   a. At least every 90 days;

   b. Immediately if discovered to be compromised or one suspects a password has been compromised;

   c. Immediately if discovered to be in noncompliance with this policy or upon direction from management.

9. Do not reuse a password you have used any of the last 8 times you have changed your password, or more recently than 2 years from when you last used the password.

10. If a determination is made that a password has been compromised or is not in compliance with this policy, and if the password is not immediately changed, the account must be temporarily suspended until the password is changed.

11. Passwords for servers, mainframes, telecommunications devices (such as routers and switches) and devices used for IT security functions (such as firewalls, intrusion detections, and audit logging) must be encrypted when stored electronically.

12. Passwords, other than single-use (one-time) passwords, must be encrypted when transmitted across a wide area network or the Internet.

ATTACHMENT C
EMRS Report Sample